BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

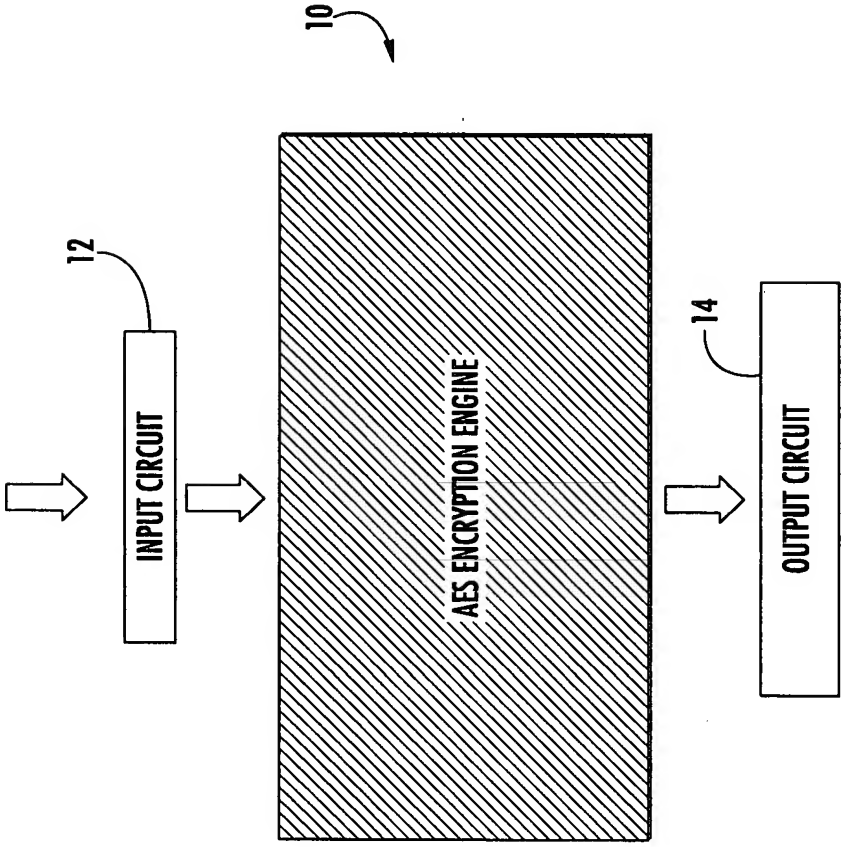


FIG. 1

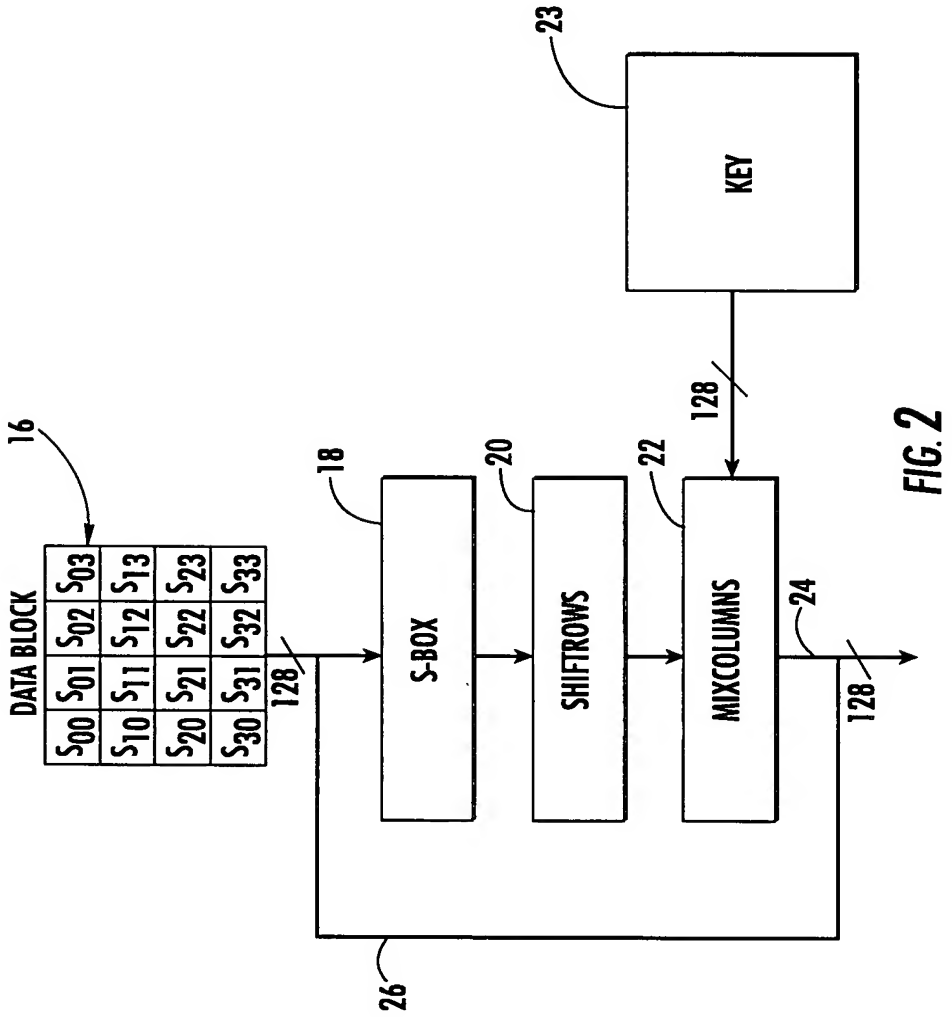
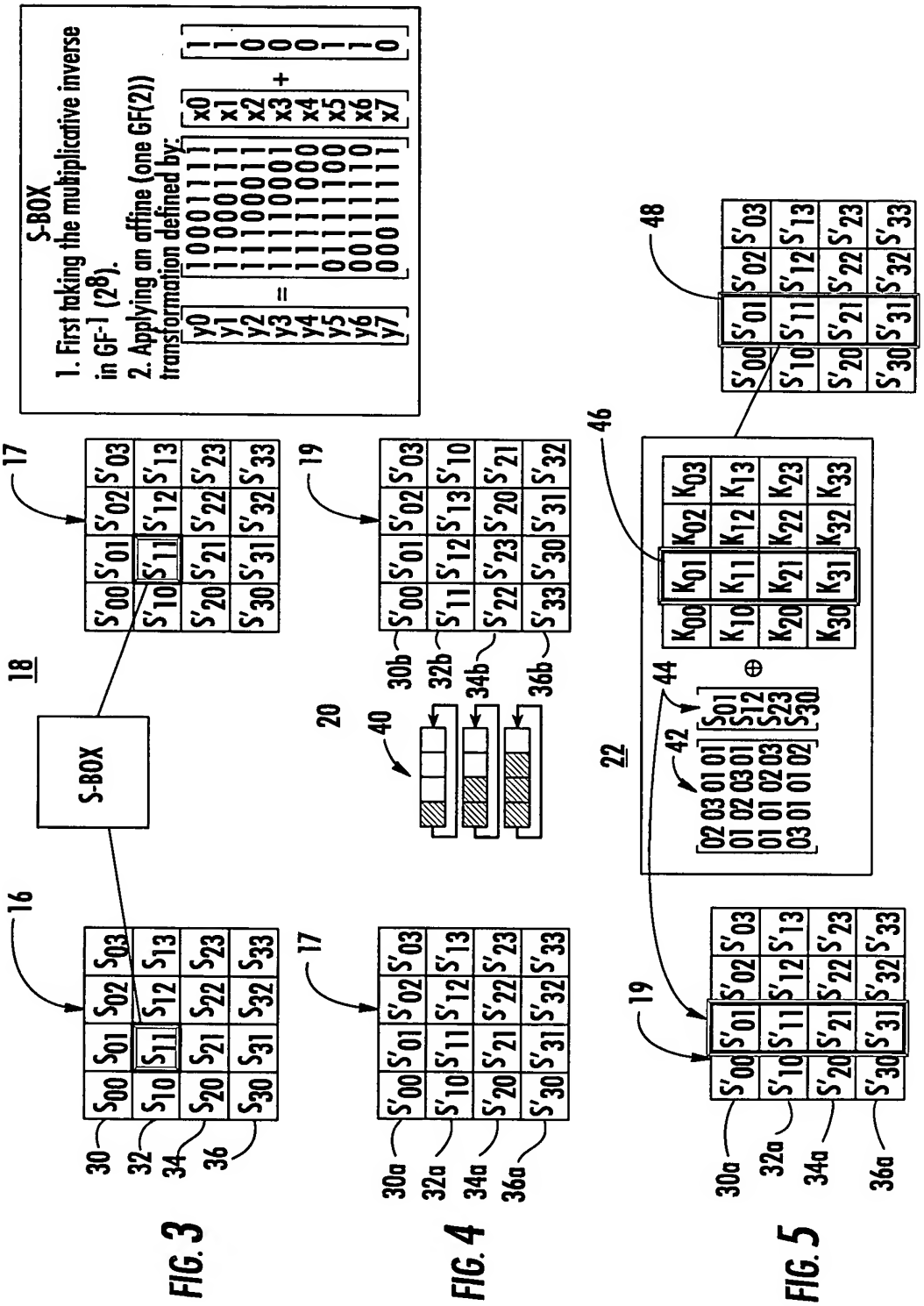

23
KEY
128
16
18
20
22
DATA BLOCK
S03 S13 S23 S33
S02 S12 S22 S32
S01 S11 S21 S31
S00 S10 S20 S30
128
S-BOX
SHIFTROWS
MIXCOLUMNS
24
128
26

FIG. 2

3/15


S-BOX
1. First taking the multiplicative inverse in GF-1 (28).
2. Applying an affine (one GF(2)) transformation defined by:
y0 y1 y2 y3 y4 y5 y6 y7 = 10001111 11000111 11100011 11110001 11111000 01111100 00111110 00011111 x0 x1 x2 x3 x4 x5 x6 x7 + 1 1 0 0 0 1 1 0
17
18
19
20
S-BOX
30b 32b 34b 36b
40
16
30 32 34 36
17
30a 32a 34a 36a
FIG. 3
FIG. 4
46
48
22
42
44
02 03 01 01
01 02 03 01
01 01 02 03
03 01 01 02
19
30a 32a 34a 36a
FIG. 5

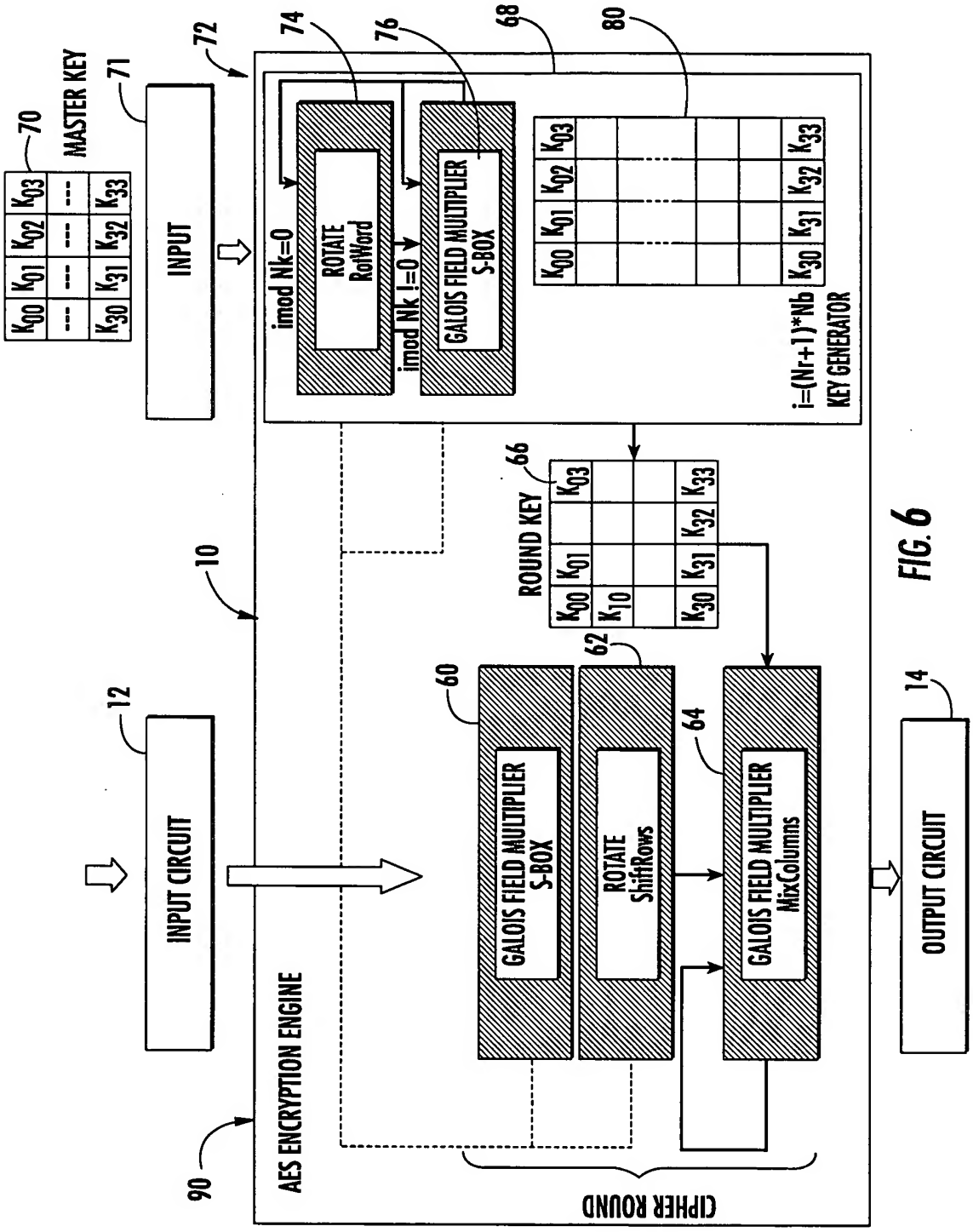

MASTER KEY
70
71
72
74
76
68
80
INPUT
imod Nk=0
ROTATE RotWord
imod Nk !=0
GALOIS FIELD MULTIPLIER S-BOX
i=(Nr+1)*Nb
KEY GENERATOR
ROUND KEY
66
10
12
60
62
64
14
INPUT CIRCUIT
GALOIS FIELD MULTIPLIER S-BOX
ROTATE ShiftRows
GALOIS FIELD MULTIPLIER MixColumns
OUTPUT CIRCUIT
90
AES ENCRYPTION ENGINE
CIPHER ROUND

FIG. 6

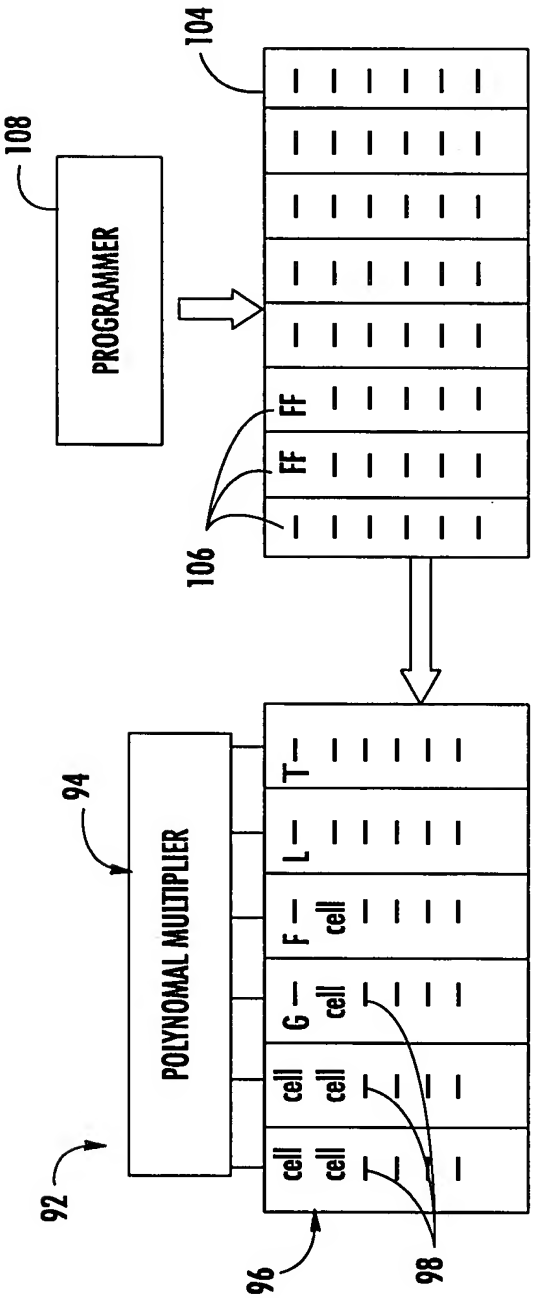

104
108
PROGRAMMER
FF
FF
106
94
POLYNOMAL MULTIPLIER
T
L
F
cell
G
cell
cell
cell
cell
cell
92
96
98

FIG. 7

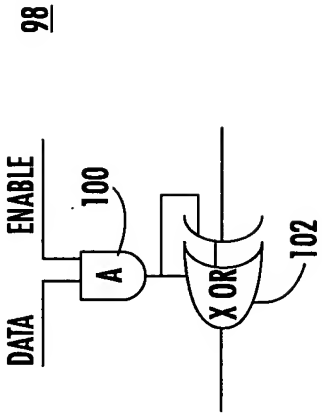

98
ENABLE
100
DATA
A
X OR
102

FIG. 8

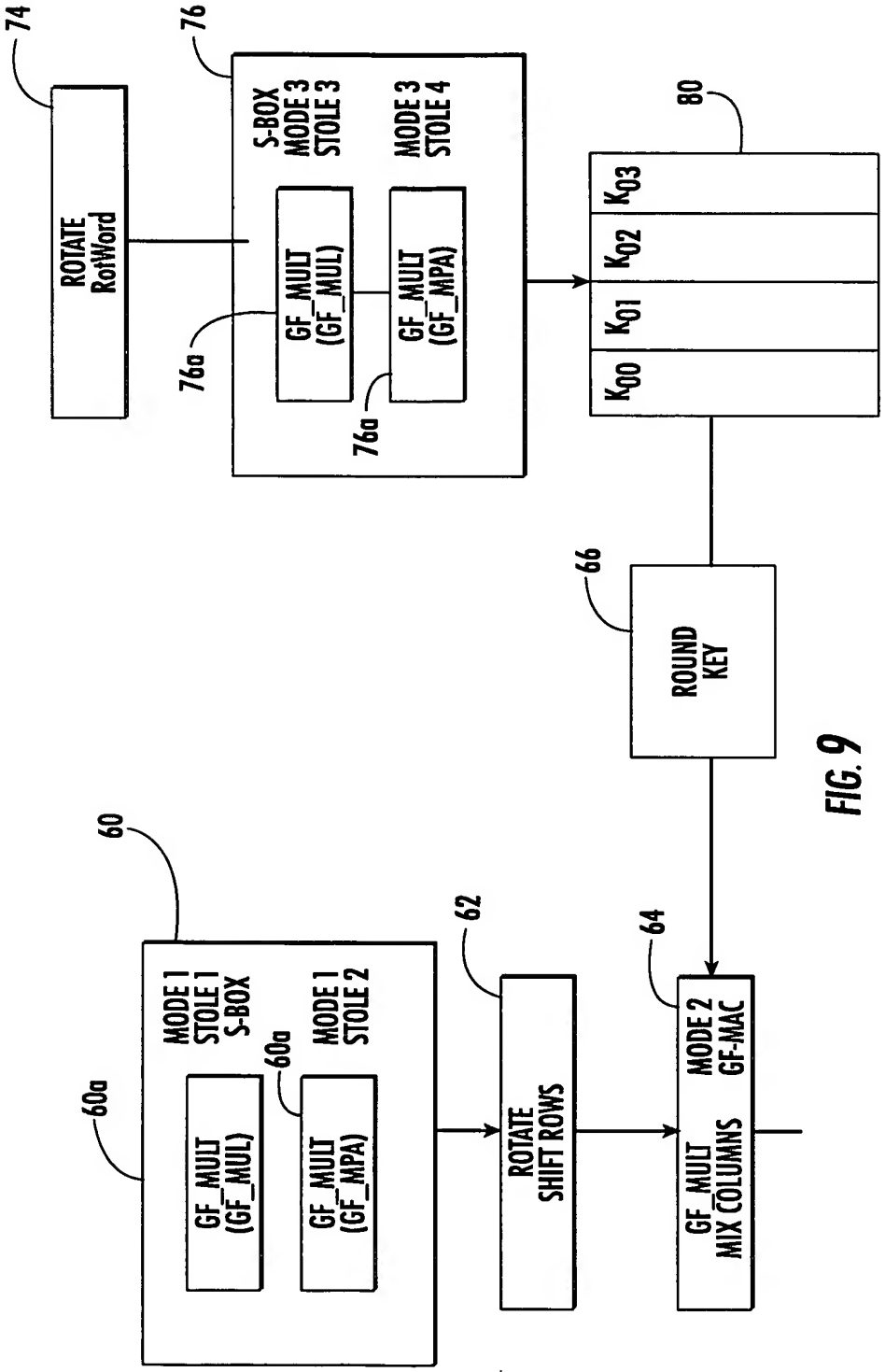

74
76
ROTATE
RotWord
S-BOX
MODE 3
STOLE 3
MODE 3
STOLE 4
GF_MULT
(GF_MUL)
GF_MULT
(GF_MPA)
76a
76a
80
K03
K02
K01
K00
66
ROUND
KEY
60
MODE 1
STOLE 1
S-BOX
MODE 1
STOLE 2
60a
60a
GF_MULT
(GF_MUL)
GF_MULT
(GF_MPA)
62
ROTATE
SHIFT ROWS
64
MODE 2
GF-MAC
GF_MULT
MIX COLUMNS

FIG. 9

7/15

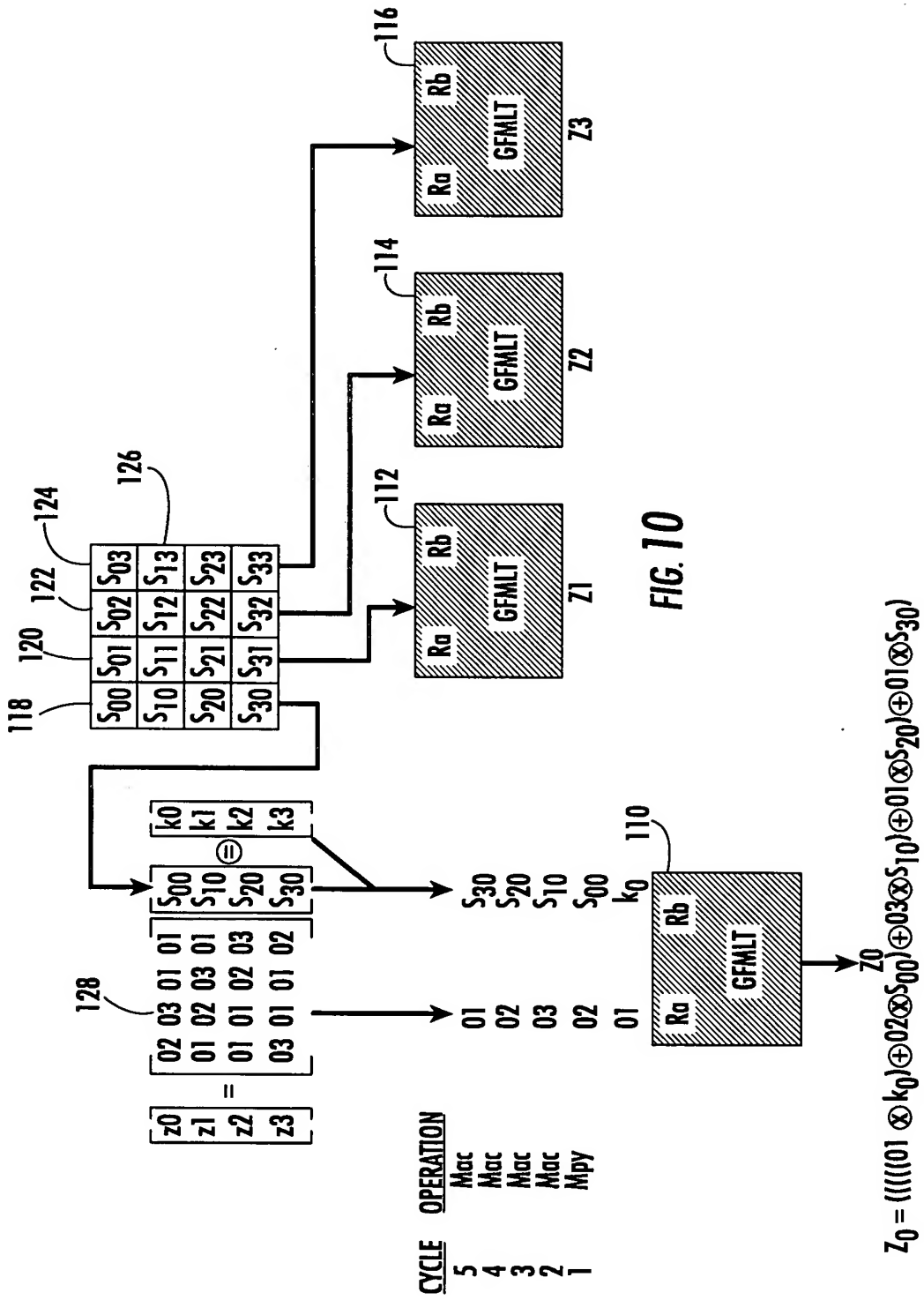

116
114
112
126
124
122
120
118
128
110
GFMLT
Ra
Rb
Z3
Z2
Z1
Z0
CYCLE
OPERATION
5 Mac
4 Mac
3 Mac
2 Mac
1 Mpy
$Z_0 = ((((01 \otimes k_0) \oplus 02 \otimes S_{00}) \oplus 03 \otimes S_{10}) \oplus 01 \otimes S_{20}) \oplus 01 \otimes S_{30})$

FIG. 10

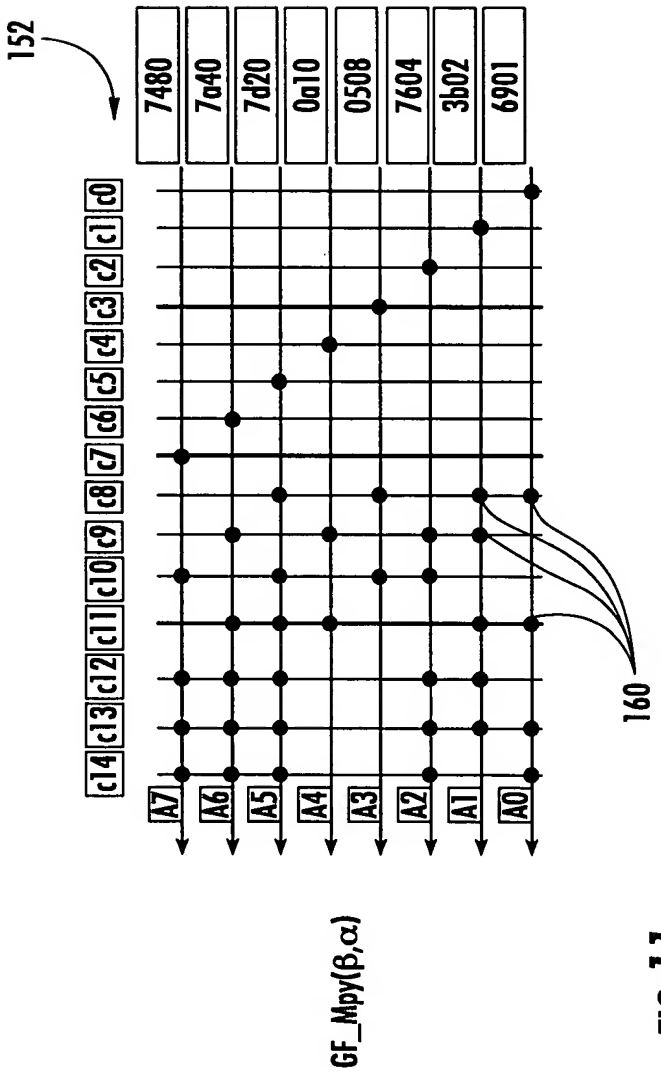
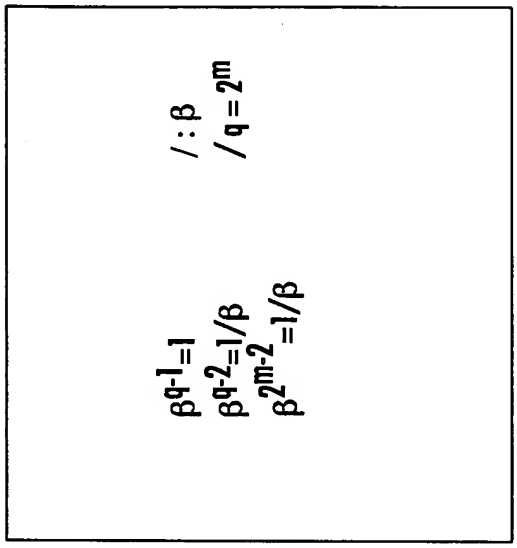

152
7480
7a40
7d20
0a10
0508
7604
3b02
6901
c0
c1
c2
c3
c4
c5
c6
c7
c8
c9
c10
c11
c12
c13
c14
A7
A6
A5
A4
A3
A2
A1
A0
160
GF_Mpy(β,α)

FIG. 11

9/15


/ : β
/ q = 2^m
β^(q-1)=1
β^(q-2)=1/β
β^(2^m-2)=1/β

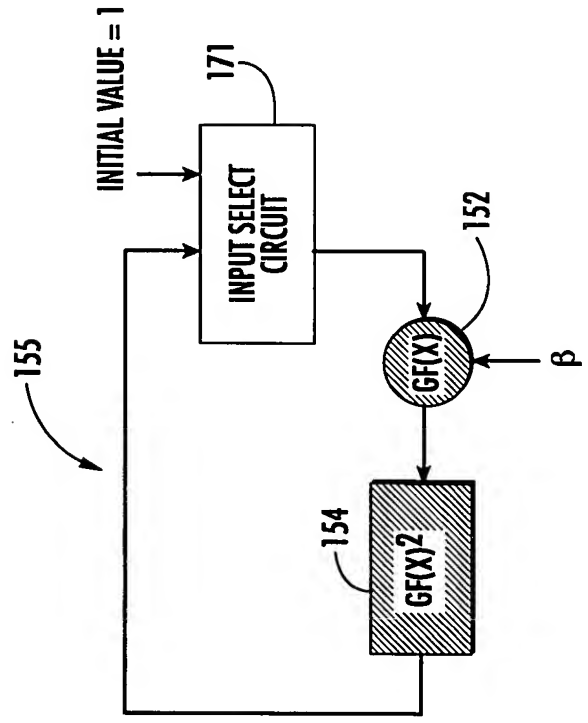

INITIAL VALUE = 1
171
INPUT SELECT CIRCUIT
152
GF(X)
β
155
154
GF(X)^2

FIG. 12

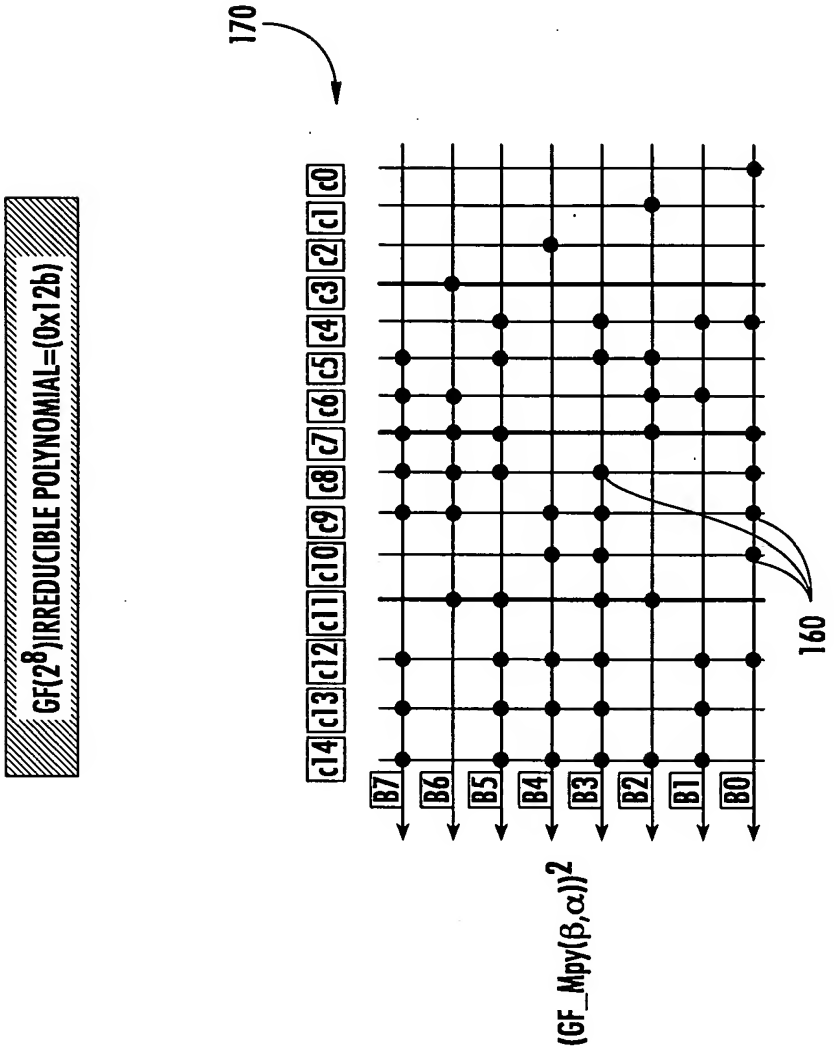

170
GF(2^8)IRREDUCIBLE POLYNOMIAL=(0x12b)
c14 c13 c12 c11 c10 c9 c8 c7 c6 c5 c4 c3 c2 c1 c0
B7 B6 B5 B4 B3 B2 B1 B0
160
(GF_Mpy(β,α))^2

FIG. 13

11/15

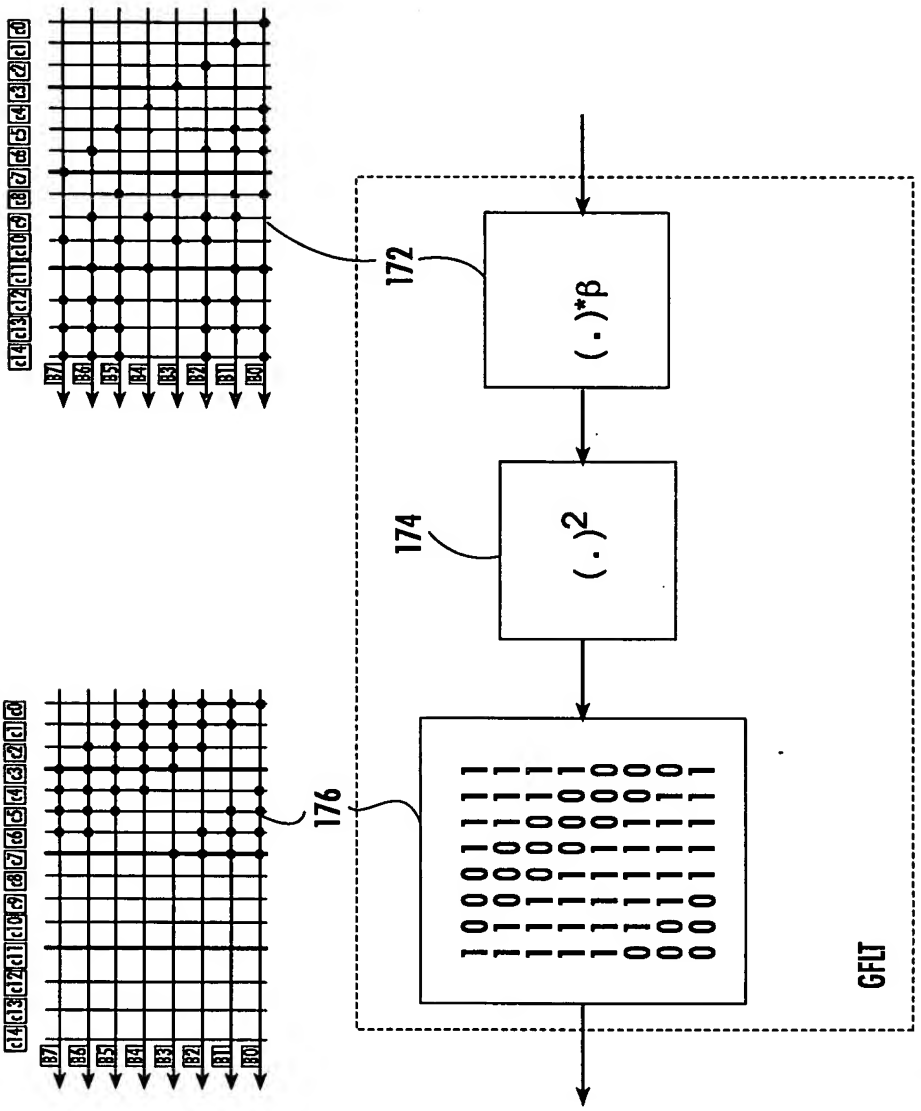


FIG. 14

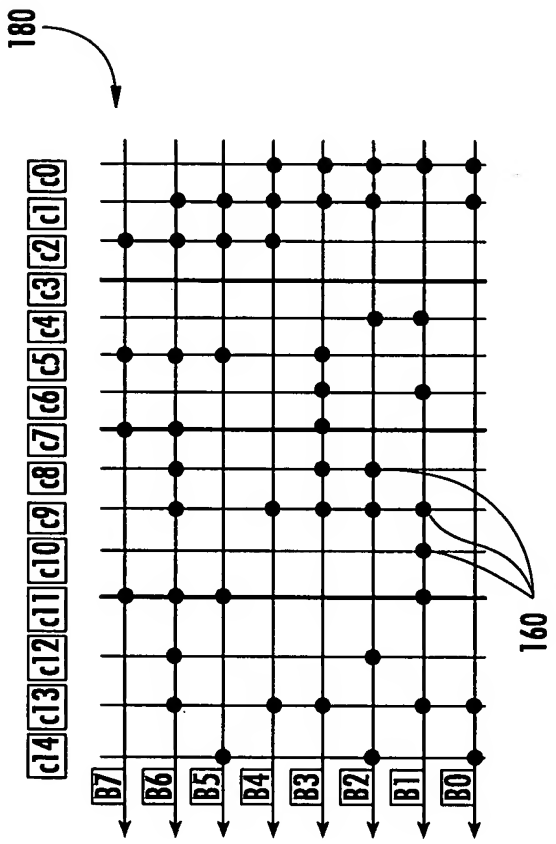

180
c0
c1
c2
c3
c4
c5
c6
c7
c8
c9
c10
c11
c12
c13
c14
B7
B6
B5
B4
B3
B2
B1
B0
160

FIG. 15

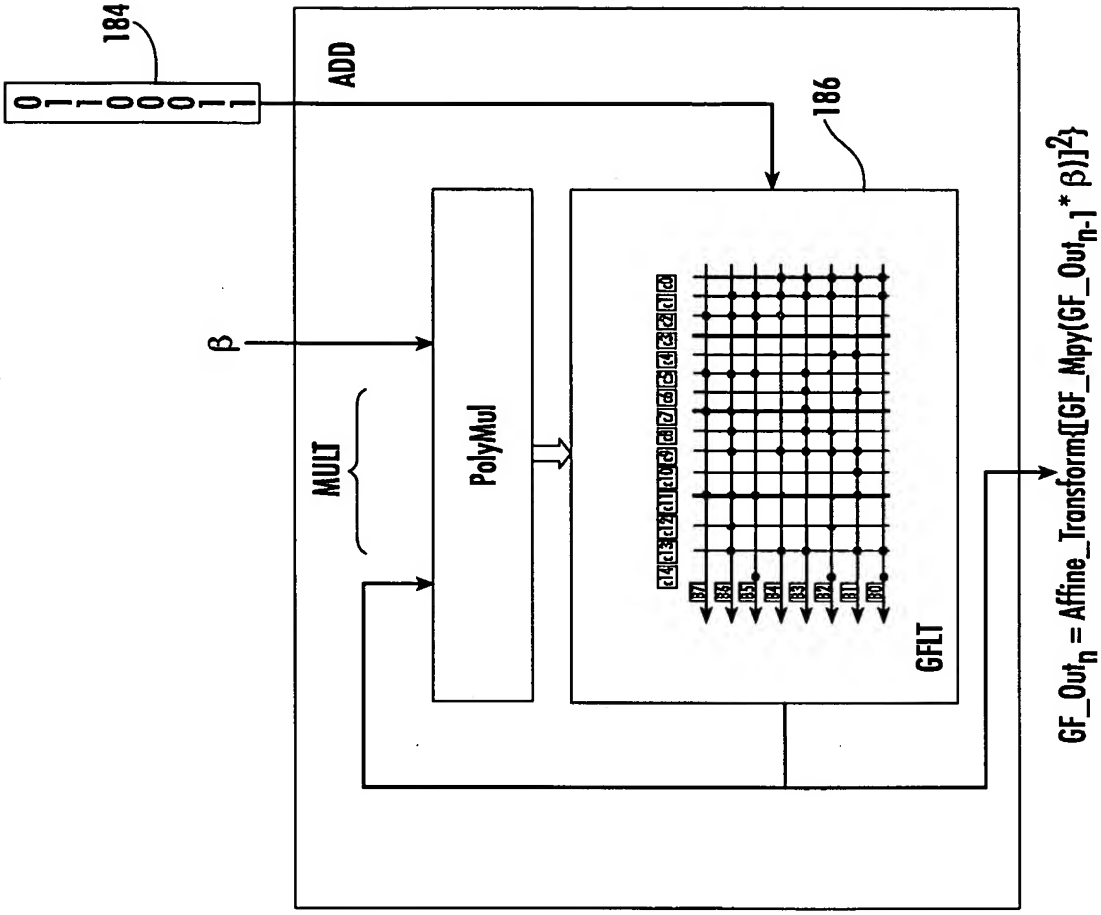

184
0 1 0 0 0 1
ADD
186
β
MULT
PolyMul
GFLT
$GF\_Out_n = Affine\_Transform\{[GF\_Mpy(GF\_Out_{n-1} * \beta)]^2\}$

FIG. 16

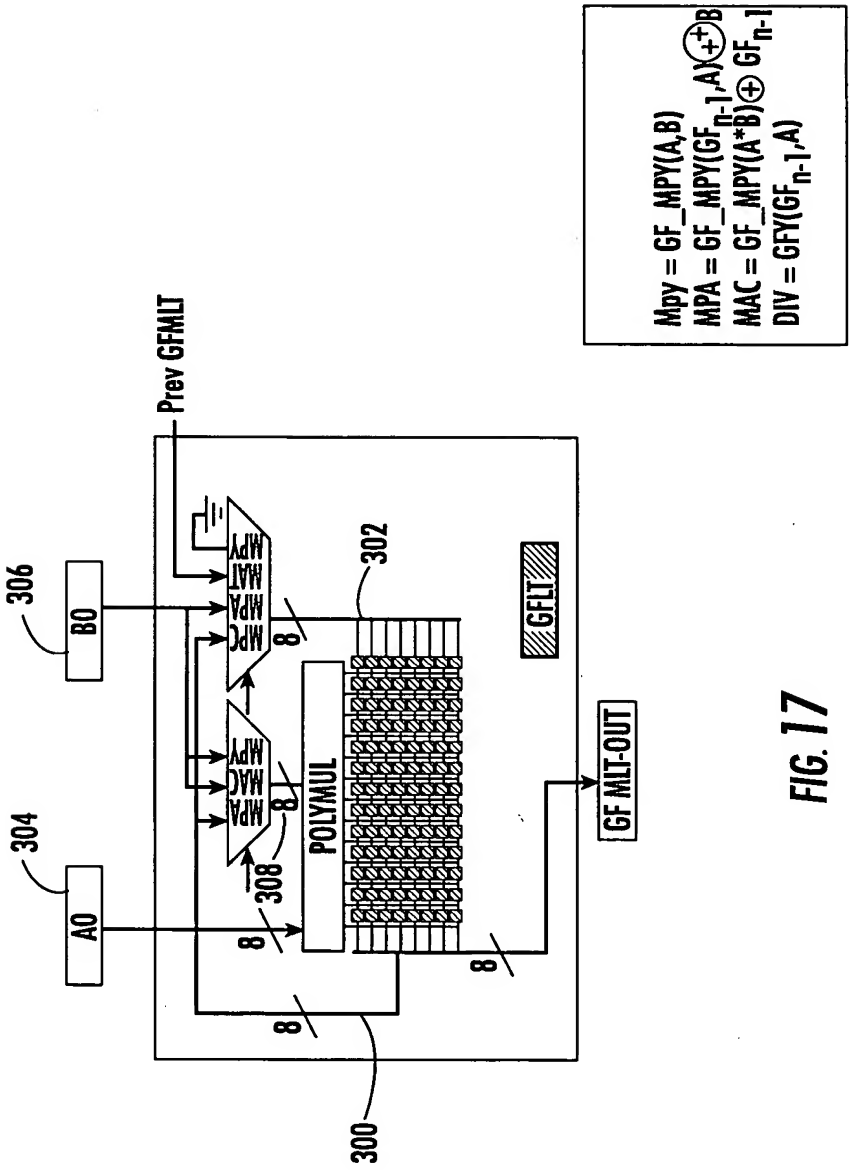

Mpy = GF_MPY(A,B)
MPA = GF_MPY(GF$_{n-1}$,A)⊕B
MAC = GF_MPY(A*B)⊕ GF$_{n-1}$
DIV = GFY(GF$_{n-1}$,A)
Prev GFMLT
306
B0
304
A0
MPY
MAT
MPA
MPC
MPY
MAC
MPA
8
308
POLYMUL
302
GFLIT
GF MLT-OUT
300

FIG. 17

15/15

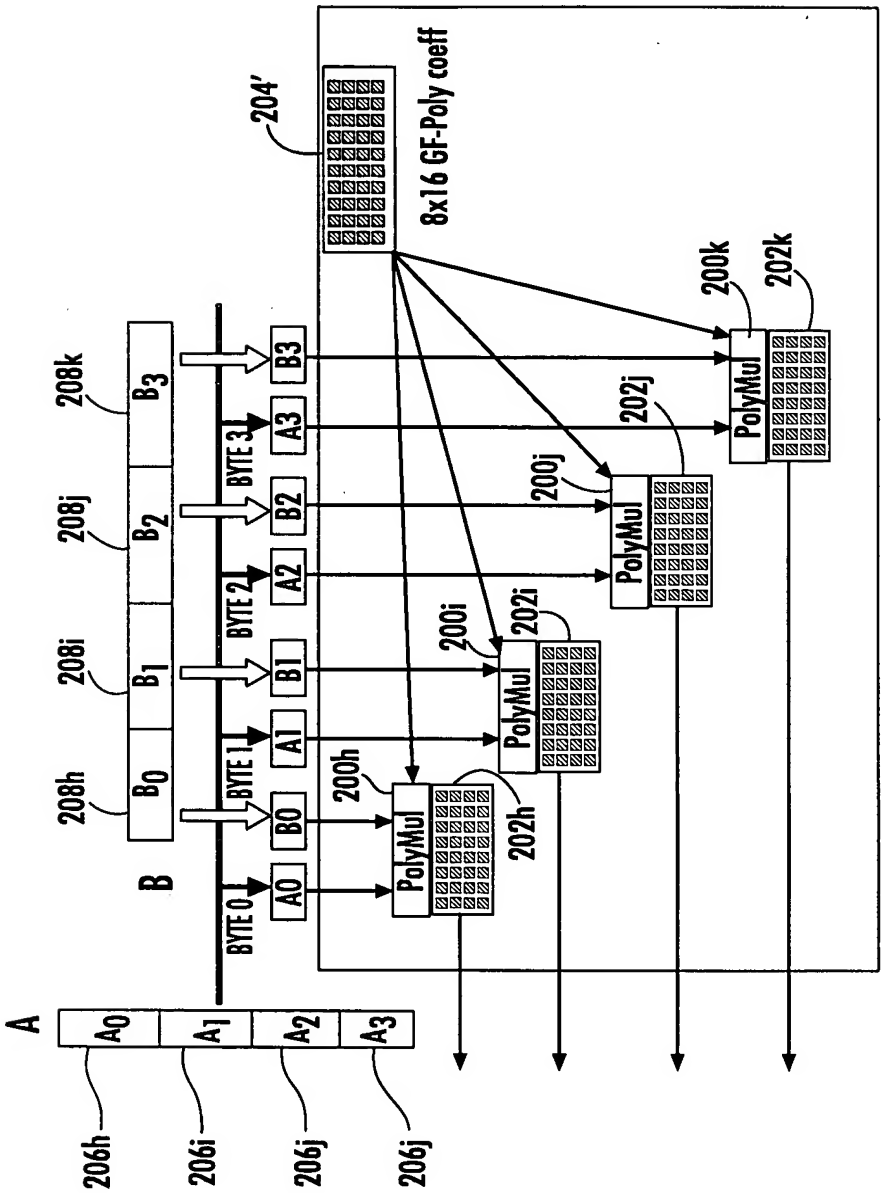

204'
8x16 GF-Poly coeff
200k
202k
202j
200j
200i
202i
200h
202h
PolyMul
208k
208j
208i
208h
B3
B2
B1
B0
B
BYTE 3
BYTE 2
BYTE 1
BYTE 0
A3
A2
A1
A0
A
206h
206i
206j
206j

FIG. 18